WELTORGANISATION FÜR GEISTIGES EIGENTUM

Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6: (11) Internationale Veröffentlichungsnummer: WO 98/26569 **A2** H04M 11/06 (43) Internationales 18. Juni 1998 (18.06.98) Veröffentlichungsdatum:

(21) Internationales Aktenzeichen:

PCT/EP97/06663

(22) Internationales Anmeldedatum:

29. November 1997

(29.11.97)

(81) Bestimmungsstaaten: AU, CA, CZ, HU, IS, JP, KR, MX, NO, NZ, PL, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

(30) Prioritätsdaten:

196 53 713.4

10. Dezember 1996 (10.12.96)

(71) Anmelder alle Bestimmungsstaaten ausser AG DEUTSCHE TELEKOM [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder: und

(75) Erfinder/Anmelder (nur für US): STOLZ, Helmut [DE/DE]; Am Gensberge 12, D-57080 Siegen (DE).

(74) Anwalt: KAMPFENKEL, Klaus; Sonnenberger Strasse 100, D-65193 Wiesbaden (DE).

Veröffentlicht

Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD AND DEVICE FOR THE REMOTE OPERATION AND REMOTE CONTROL OF SYSTEMS AND APPARATUS VIA A TELEPHONE NETWORK

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM FERNBEDIENEN UND FERNSTEUERN VON EINRICHTUNGEN UND GERÄTEN ÜBER EIN TELEFONNETZ

(57) Abstract

The known methods and devices, which resemble the remote access systems for answering machines, do not provide sufficient protection against copying and manipulation. With the modified method, the establishment of connections between the base station and the adapters is made dependent on a unilateral authentication process. Before making his DTMF (dual tone multi-frequency dialling) selection, the user identifies himself with respect to the base station using coded data which comprise a "key" and a "secret" and are tested there for conformity with stored data concerning authorized persons. If conformity exists, readiness for connection to an adapter is acknowledged by means of a first ready signal. It is only then that, in a similarly coded manner, the adapter and type of actuation, which are acknowledged by status signals or a further ready signal, are selected. The method even enables critical functions with greater demands as concerns security to be remotely controlled via the public telephone network, for which dedicated lines would otherwise be necessary.

(57) Zusammenfassung

Die bekannten Verfahren und Vorrichtungen, die den Fernabfragen für Anrufbeantwortern ähneln, vermeiden das Kopieren und Manipulieren nicht sicher genug. Bei dem veränderten Verfahren wird das Herstellen von Verbindungen von der Zentralstation zu den Adaptern von einer einseitigen Authentikation abhängig gemacht, bei der sich der Benutzer gegenüber der Zentralstation vor seiner MFV-Wahl mit einer aus "Schlüssel" und "Geheimnis" gebildeten verschlüsselten Information ausweist, welche dort auf Übereinstimmung mit gespeicherten Information der Berechtigten geprüft und, falls sie gegeben ist, die Bereitschaft zur Verbindung mit einem Adapter mit einem ersten Bereitsignal quittiert wird, daß erst danach, ebenso verschlüsselt, Adapter und Betätigungsart gewählt werden, die durch Zustandssignale bzw. ein weiteres Bereitsignal quittiert werden. Mit dem Verfahren wird die Fernsteuerung auch kritischer Funktionen mit erhöhten Sicherheitsanforderungen über das öffentliche Telefonnetz ermöglicht, für die sonst fest geschaltete Leitungen erforderlich sind.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

ES FI	Spanien		Lesotho	SI	Slowenien
	Finnland	LS LT	Litauen	SK	Slowakei
FR	Frankreich	LU	Luxemburg	SN	Senegal
GA	Gabun	LV	Lettland	SZ	Swasiland
GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
GE	Georgien	MD	Republik Moldau	TG	Togo
GH	Ghana	MG	Madagaskar	ТĴ	Tadschikistan
GN	Guinea	MK	Die ehemalige jugoslawische	TM	Turkmenistan
	Griechenland	IVI	Republik Mazedonien	TR	Türkei
GR		ML	Mali	TT	Trinidad und Tobago
HU	Ungarn	-		UA	Ukraine
IE	Irland	MN	Mongolei		
IL	Israel	MR	Mauretanien	UG	Uganda
IS	Island	MW	Malawi	US	Vereinigte Staaten von
IT	Italien	MX	Mexiko		Amerika
JP	Japan	NE	Niger	$\mathbf{U}\mathbf{Z}$	Usbekistan
KE	Kenia	NL	Niederlande	VN	Vietnam
KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
KP	Demokratische Volksrepublik	NZ	Neuseeland	ZW	Zimbabwe
	Korea	PL	Polen		
KR	Republik Korea	PT	Portugal		
KZ	Kasachstan	RO	Rumänien		
LC	St. Lucia	RU	Russische Föderation		
LI	Liechtenstein	SD	Sudan		
LK	Sri Lanka	SE	Schweden		
LR	Liberia	SG	Singapur		
	LI LK	LI Liechtenstein LK Sri Lanka	LI Liechtenstein SD LK Sri Lanka SE	LI Liechtenstein SD Sudan LK Sri Lanka SE Schweden	LI Liechtenstein SD Sudan LK Sri Lanka SE Schweden

Verfahren und Vorrichtung zum Fernbedienen und Fernsteuern von Einrichtungen und Geräten über ein Telefonnetz

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren der im Oberbegriff des Patentanspruchs 1 näher bezeichneten Art, sowie auf eine Vorrichtung der im Oberbegriff des Patentanspruchs 3 definierten Art. Derartige Verfahren und Vorrichtungen sind z. B aus UK Patent Application GB 2 2230 163 A; DE 36 24 162 A1 und DE 42 28 071 A1 bekannt.

Diese Verfahren und Vorrichtungen dienen dazu, beliebige Einrichtungen und Geräte in Haushalten, Büroräumen, Unternehmungen usw. über ein Telefonnetz zu bedienen und zu steuern. Verfahrensweise, Aufbau und der Autorisierungsmechanismus ähneln denen, die bei der Fernabfrage und Steuerung von Telefon-Anrufbeantwortern üblich sind.

Als Autorisierungsmechanismus wird ein Password-Verfahren verwendet, beispielsweise eine Ziffer als MFV-Wahlzeichen, und die Nutzinformationen werden im Klartext übermittelt. Ein unautorisierter Benutzer kann mittels bekannter Verfahren die Nutzinformationen manipulieren. Außerdem kann er sich in den Besitz der Autorisierungsmechanismen bringen (durch Aufzeichnung der Kommunikation) und selbständig neue Verbindungen aufbauen, ohne den originären Benutzer persönlich zu kompromittieren.

Aufgabe der Erfindung ist es, daß nur autorisierten Benutzern ein authentischer Zugriff auf die entsprechenden Einrichtungen möglich sein soll. Die Nutzinformationen sollen vor unberechtigtem Zugriff und gezielter Manipulation geschützt werden.

2

Die Erfindung löst diese Aufgabe mit der im Kennzeichen des Patentanspruchs 1 beschriebenen Verfahrensweise.

Eine vorteilhafte Weiterbildungsmöglichkeit des Verfahrens ist im Kennzeichen des Patentanspruchs 2 angeführt.

Eine Vorrichtung, die zur Lösung dieser Aufgabe geeignet ist, ist im Kennzeichen des Patentanspruchs 3 beschrieben.

Die Erfindung wird nachfolgend anhand von Ausführungsbeispielen näher erklärt. In den zugehörigen Zeichnungen zeigen die

- Fig. 1 eine Prinzipskizze der bekannten Vergleichs lösungen,
- Fig. 2 eine Prinzipskizze einer Zentralstation und
- Fig. 3 eine Prinzipskizze einer Außenstelle eines Benutzers.

Die bekannten Vergleichslösungen, entsprechend Fig. 1, bedürfen keiner ausführlichen Erklärung, wenn sie mit der allgemein bekannten Fernabfrage eines Anrufbeantworters verglichen werden. Am Telefonendgerät des Benutzers wird, soweit dieses nicht für MFV-Wahl vorgesehen ist, ein MFV-Geber akustisch angekoppelt. Als Autorisierungsmechanismus dient die eingegebene Ziffer, durch die hier, anstelle eines Anrufbeantworters, eine Zusatzeinrichtung eingeschaltet wird. Deren ausgangsseitige Schnittstellen werden mit nachfolgenden offenen Zeichen gesteuert.

Die Zusatzeinrichtung (einer Zentralstation Z) für analoge Fernsprechanschlüsse nach Fig. 2 besteht aus einer Anschlußeinheit für Telefonnetz TAE, einem Übertrager mit Rufstromunterdrückung 12, Verstärker 13, einem Empfänger/Decodierer für die MFV-Zeichen 14, bei vorgesehener Rückinformation einem MFV-Sender DTMF (Dual Tone Multiple

Frequence) 15, einem Kleinrechner 16, einer Tastatur 17, einem Display 18 (Anzeigefeld), einem Speicher und Vergleicher 21 für verschlüsselte Berechtigungssignale, sowie Schaltgliedern a, b, bis n mit ihren Schnittstellen für die Steuerung von diversen Adaptern.

3

Eine Endeinrichtung für Benutzer besteht, entsprechend Fig. 3, aus einem Lautsprecher 1, einem Verstärker 2, einem Sender für DTMF (Dual Tone Multiple Frequence)-Zeichen 3, einer Aufnahme für Sicherheitsmodul 4, einem personalisierten Sicherheitsmodul 5, einem Kleinrechner 6, einer Tastatur 7, optional einer Anzeigeeinheit (Display) 8 und einer Batterie.

Die zur Initialisierung der einzelnen Funktionen benutzten Mehrfrequenzsender enthalten zusätzlich eine Aufnahme- und Leseeinrichtung für personalisierbare Sicherheitsmodule (SM), z. B. eine personalisierbare CPU-Chipkarte (ICC) und eine Sicherheitssoftware, um die SM anzusprechen.

Der Benutzer erhält ein personalisiertes SM. Als logischer Zugriffsschutz zum SM kann ein PIN (personal identification number)-Mechanismus verwendet werden. (Damit besteht das persönliche Identifikationsmerkmal aus den Komponenten "Wissen" und "Besitz".) Das personalisierte SM enthält unauslesbar gespeicherte individuelle kryptografische Schlüssel. Das SM verschlüsselt und entschlüsselt u. a. die Nutzinformationen und wird für die gegenseitige Authentikation Benutzer und zentrale Einrichtung verwendet.

Die zentrale Einrichtung erhält ebenfalls zusätzlich eine Aufnahme- und Leseeinrichtung für personalisierbare Sicherheitsmodule (SM), z. B. eine personalisierbare CPU-Chipkarte (ICC) und eine Sicherheitssoftware, um die SM anzusprechen.

4

Das SM im Mehrfrequenzsender und in der Zentraleinrichtung besitzen identische kryptographische Schlüssel für diesen Benutzer. Das heißt, für jede Kombination Benutzer SM und SM in der Zentraleinrichtung werden individuelle Schlüssel benutzt.

Die Informationsinhalte für Verbindungseröffnung usw. sind in der Zentraleinrichtung programmierbar.

Der Benutzer steckt sein personalisiertes Sicherheitsmodul SM (z. B. eine Chipkarte) in seinen Mehrfrequenzsender und gibt seine PIN (Personal Identifikation Number) ein. Die PIN wird zum SM gesendet und dort verifiziert. Bei richtiger PIN ist der Zugang zum SM geöffnet und am Mehrfrequenzsender wird ein akustisches oder optisches Signal gesetzt (z. B. eine Leuchtdiode oder ein Ton bestimmter Frequenz). Nun wählt der Benutzer die entsprechende Verbindung zu seiner Zentralstation (am Telefonnetz angeschlossen) und diese sendet einen ersten Bereitton. Daraufhin initiiert der Benutzer eine Verbindungseröffnungsinformation (Befehlssequenz 1). Diese Sequenz wird in seinem SM mit seinem personalisierten kryptographischen Schlüssel verschlüsselt und als verschlüsselte Information zur Zentralstation gesendet. Diese entschlüsselt die empfangene Information und vergleicht diese mit der hier gespeicherten. Bei positivem Ergebnis sendet die Zentraleinrichtung einen weiteren "Bereitton". Nun kann der Benutzer die entsprechenden Befehle initiieren, die dann nach Verschlüsselung in seinem SM zur Zentralstation gesendet werden. Diese sendet dann die Befehle an die entsprechenden Einrichtungen.

Ein möglicher Angreifer kann die verschlüsselte Information nicht gezielt verändern, jedoch wird u. U. eine Veränderung der Nutzinformation vom Benutzer nicht bemerkt. Dieser Mangel kann zusätzlich wie folgt abgestellt werden:

5

Nach Empfang des zweiten "Bereittons" initiiert der Benutzer die entsprechenden Befehle. Diese werden im Klartext und zusätzlich nach Verschlüsselung in seinem SM verschlüsselt zur Zentralstation gesendet. Diese bildet nun von der Klartextinformation nochmals das verschlüsselte Produkt und vergleicht dieses mit dem empfangenen verschlüsselten Produkt und gibt den entsprechenden Befehl nur bei positiven Prüfergebnis an die entspr. Einrichtungen weiter. Mit einer Rückmeldung der Befehle und Ergebnisse von der Zentralstation Z zum Benutzer X kann eine weitere Erhöhung der Sicherheit erreicht werden.

6

Patentansprüche

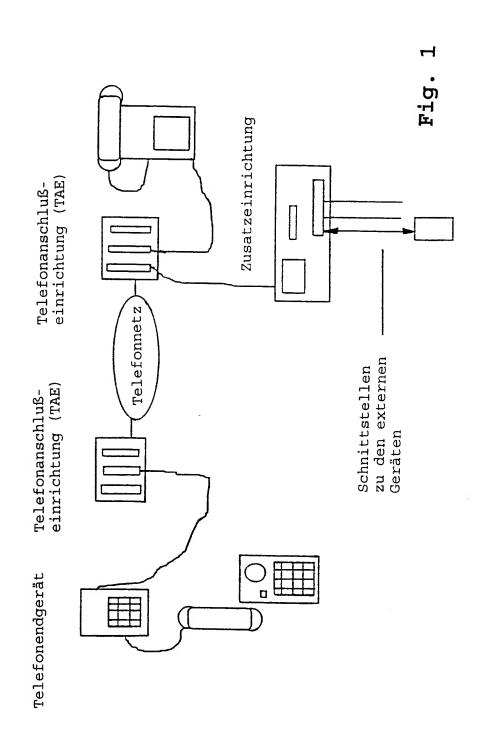
WO 98/26569

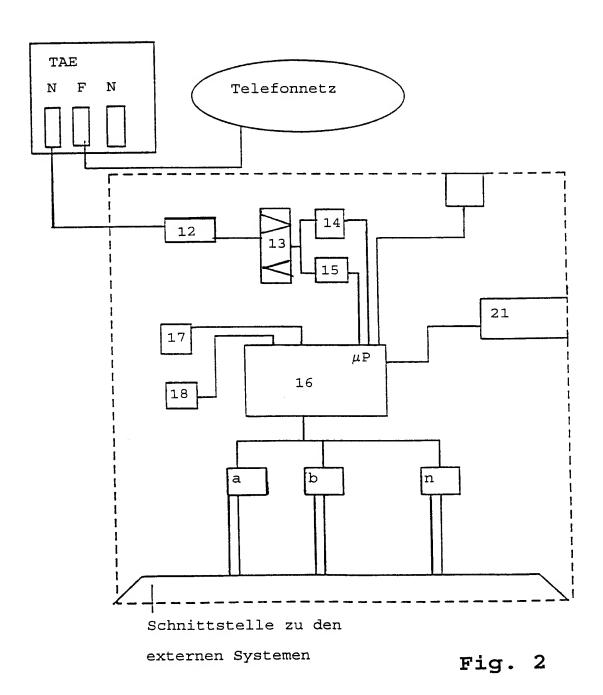
- 1. Verfahren zum Fernbedienen und Fernsteuern von Einrichtungen und Geräten über ein Telefonnetz, bei dem von beliebigen Anschlußstellen aus Verbindungen zu einer Zentralstation hergestellt werden, über die, mittels MFV-Wahl und Autorisierung, den Einrichtungen und Geräten zugeordnete Adapter angesteuert werden, die Zustandsabfragen bzw. Betätigungen initileren, dadurch gekennzeichnet, das Herstellen von Verbindungen von der Zentralstation zu den Adaptern von einer einseitigen Authentikation abhängig gemacht wird, bei der sich der Benutzer gegenüber der Zentralstation vor seiner MFV-Wahl mit einer aus "Schlüssel" und "Geheimnis" gebildeten verschlüsselten Information ausweist, welche von dieser durch einen Vergleich mit einer gespeicherten Information der Berechtigten auf Übereinstimmung geprüft und, falls sie gegeben ist, die Bereitschaft zur Verbindung mit einem Adapter mit einem ersten Bereitsignal quittiert wird, daß danach, ebenso verschlüsselt, Adapter und Betätigungsart gewählt werden, die durch Zustandssignale bzw. ein weiteres Bereitsignal quittiert werden.
- 2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß nach Empfang des zweiten Bereitsignal vom Benutzer die Befehle im Klartext und zusätzlich nach Verschlüsselung in seinem SM verschlüsselt zur Zentralstation gesendet werden und daß diese vor der Weitergabe des Befehls an das Adapter von der Klartextinformation das verschlüsselte Produkt bildet und dieses mit dem empfangenen

7

verschlüsselten Produkt vergleicht und den Befehl nur bei positiven Prüfergebnis weitergibt .

3. Vorrichtung zum Fernbedienen und Fernsteuern von Einrichtungen und Geräten über ein Telefonnetz, bei dem einer Zentralstation und den Einrichtungen und Geräten Adapter zugeordnet sind, die von beliebigen Anschlußstellen aus mittels MFV-Wahlvorrichtung anwählbar und nach Autorisierung initiierbar sind, dadurch gekennzeichnet, daß den Benutzern bzw. deren Stationen Sender für DTMF (Dual Tone Multiple Frequence)-Zeichen (3), eine Aufnahme für ein Sicherheitsmodul (4), ein personalisierter Sicherheitsmodul (5), ein Kleinrechner (6), eine Tastatur (7), und optional eine Anzeigeeinheit (Display) (8) und der Zentralstation Speicher und Vergleicher für verschlüsselte Informationen zugeordnet sind, welche Verbindungen zu den Adaptern nur nach erfolgreichem Vergleich mit einer von einer Außenstelle gesendeten verschlüsselten Information freigeben, die dort in einem personalisierten Sicherheitsmodul SM in Verknüpfung mit einem personengebundenen Geheimnis, insbesondere PIN (Personal Identification Number) gebildet und in MFV-Informationen umgesetzt ist.





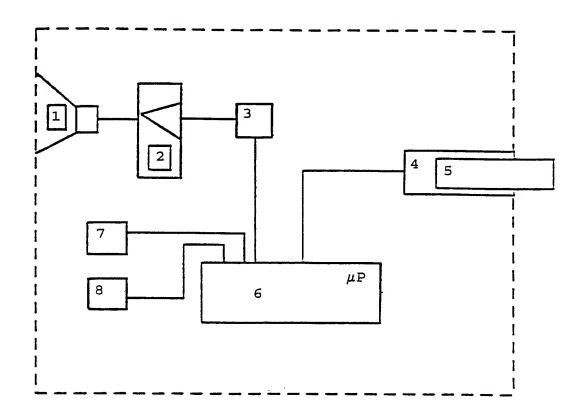


Fig. 3

WELTORGANISATION FUR GEISTIGES EIGENTUM

Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6:

H04M 11/00, H04L 9/32

(11) Internationale Veröffentlichungsnummer:

WO 98/26569

(43) Internationales Veröffentlichungsdatum:

18. Juni 1998 (18.06.98)

(21) Internationales Aktenzeichen:

PCT/EP97/06663

A3

(22) Internationales Anmeldedatum:

29. November 1997

(29.11.97)

(81) Bestimmungsstaaten: AU, CA, CZ, HU, IS, JP, KR, MX, NO, NZ, PL, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT,

SE).

(30) Prioritätsdaten:

196 53 713.4

10. Dezember 1996 (10.12.96) DE Veröffentlicht

Mit internationalem Recherchenbericht.

(71) Anmelder (für alle Bestimmungsstaaten ausser US): **DEUTSCHE** TELEKOM AG [DE/DE];

Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

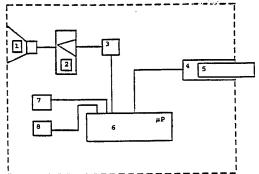
(75) Erfinder/Anmelder (nur für US): STOLZ, Helmut [DE/DE]; Am Gensberge 12, D-57080 Siegen (DE).

(74) Anwalt: KAMPFENKEL, Klaus; Sonnenberger Strasse 100, D-65193 Wiesbaden (DE).

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 29. Oktober 1998 (29.10.98)

(54) Title: METHOD AND DEVICE FOR THE REMOTE OPERATION AND REMOTE CONTROL OF SYSTEMS AND APPARATUS VIA A TELEPHONE NETWORK

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM FERNBEDIENEN UND FERNSTEUERN VON EINRICHTUNGEN UND GERÄTEN ÜBER EIN TELEFONNETZ



(57) Abstract

The invention concerns a method wherein the establishment of connections between the base station and the adapters is made dependent on a unilateral authentication process. Before making his DTMF (dual tone multi-frequency dialling) selection, the user identifies himself with respect to the base station using coded data which comprise a "key" and a "secret" and are tested there for conformity with stored data concerning authorized persons. If conformity exists, readiness for connection to an adapter is acknowledged by means of a first ready signal. It is only then that, in a similarly coded manner, the adapter and type of actuation, which are acknowledged by status signals or a further ready signal, are selected. The method even enables critical functions with greater demands as concerns security to be remotely controlled via the public telephone network, for which dedicated lines would otherwise be necessary.

(57) Zusammenfassung

Bei dem Verfahren wird das Herstellen von Verbindungen von der Zentralstation zu den Adaptern von einer einseitigen Authentikation abhängig gemacht, bei der sich der Benutzer gegenüber der Zentralstation vor seiner MFV-Wahl mit einer aus "Schlüssel" und "Geheimnis" gebildeten verschlüsselten Information ausweist, welche dort auf Übereinstimmung mit gespeicherten Information der Berechtigten geprüft und, falls sie gegeben ist, die Bereitschaft zur Verbindung mit einem Adapter mit einem ersten Bereitsignal quittiert wird, daß erst danach, ebenso verschlüsselt, Adapter und Betätigungsart gewählt werden, die durch Zustandssignale bzw. ein weiteres Bereitsignal quittiert werden. Mit dem Verfahren wird die Fernsteuerung auch kritischer Funktionen mit erhöhten Sicherheitsanforderungen über das öffentliche Telefonnetz ermöglicht, für die sonst fest geschaltete Leitungen erforderlich sind.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
вв	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland		Republik Mazedonien	TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	\mathbf{UG}	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von
CA	Kanada	IT	Italien	MX	Mexiko		Amerika
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik	NZ	Neuseeland	$\mathbf{z}\mathbf{w}$	Zimbabwe
CM	Kamerun		Korea	PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	\mathbf{SG}	Singapur		

INTERNATIONAL SEARCH REPORT

al Application No

PCT/EP 97/06663 CLASSIFICATION OF SUBJECT MATTER PC 6 H04M11/00 H04L IPC 6 H04L9/32 According to International Patent Classification (IPC) or to both national classification and IPC **B. FIELDS SEARCHED** Minimum documentation searched (classification system followed by classification symbols) IPC-6 HO4M HO4L Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practical, search terms used) C. DOCUMENTS CONSIDERED TO BE RELEVANT Citation of document, with indication, where appropriate, of the relevant passages Relevant to claim No. FR 2 680 592 A (TOKYO SHIBAURA ELECTRIC 1,3 CO) 26 February 1993 see abstract see page 1, line 1 - page 12, line 18 see figures 1,2 Υ DE 43 25 459 A (C2S GMBH CRYPTOGRAFISCHE 1,3 SICHE) 9 February 1995 see the whole document US 5 119 412 A (ATTALLAH ARNALDO) 2 June Α 1,3 1992 see abstract see column 1, line 1 - column 5, line 44 see column 9, line 17 - column 11, line 2 Further documents are listed in the continuation of box C. Patent family members are listed in annex. ° Special categories of cited documents : "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the "A" document defining the general state of the art which is not considered to be of particular relevance invention earlier document but published on or after the international "X" document of particular relevance; the claimed invention filing date cannot be considered novel or cannot be considered to document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified) involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the "O" document referring to an oral disclosure, use, exhibition or document is combined with one or more other such docu ments, such combination being obvious to a person skilled document published prior to the international filing date but later than the priority date claimed "&" document member of the same patent family Date of mailing of the international search report Date of the actual completion of theinternational search 10 June 1998 17/06/1998 Name and mailing address of the ISA Authorized officer European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,

Fax: (+31-70) 340-3016

5

Lievens, K

INTERNATIONAL SEARCH REPORT

Intern. al Application No PCT/EP 97/06663

(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT	
ttegory of Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
EP 0 637 004 A (NEDERLAND PTT) 1 February 1995 see abstract see column 4. line 12 - line 29	1-3
see column 4, line 12 - line 29 see column 5, line 42 - column 9, line 21	

INTERNATIONAL SEARCH REPORT

unormation on patent family members

Interna al Application No
PCT/EP 97/06663

Patent docum cited in search r		Publication date		Patent family member(s)	Publication date
FR 268059	2 A	26-02-1993	JP JP DE	5054207 A 5061508 A 4212200 A	05-03-1993 12-03-1993 25-02-1993
DE 432545	9 A	09-02-1995	NONE		
US 511941	2 A	02-06-1992	NONE	,	
EP 063700	4 A	01-02-1995	NL AT CA DE DE DK EP ES	9301271 A 158432 T 2128355 A 69405664 D 69405664 T 637004 T 0775991 A 2107090 T	16-02-1995 15-10-1997 21-01-1995 23-10-1997 19-03-1998 14-04-1998 28-05-1997 16-11-1997

INTERNATIONALER RECHERCHENBERICHT

Interna ales Aktenzeichen PCT/EP 97/06663

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES IPK 6 H04M11/00 H04L9/32							
Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK							
	RCHIERTE GEBIETE rter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbo	e)					
IPK-6	HO4M HO4L	,					
Recherchier	rte aber nicht zum Mindestprüfstoffgehörende Veröffentlichungen, so	weit diese unter die recherchierten Gebiete	fallen				
Während de	er internationalen Recherche konsultierte elektronische Datenbank (N.	ame der Datenbank und evtl. verwendete S	Suchbegriffe)				
	SENTLICH ANGESEHENE UNTERLAGEN						
Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe	der in Betracht kommenden Teile	Betr. Anspruch Nr.				
Υ	FR 2 680 592 A (TOKYO SHIBAURA EL CO) 26.Februar 1993 siehe Zusammenfassung siehe Seite 1, Zeile 1 - Seite 12	1,3					
	18 siehe Abbildungen 1,2						
Υ	DE 43 25 459 A (C2S GMBH CRYPTOGR	1,3					
А	SICHE) 9.Februar 1995 siehe das ganze Dokument 	2					
Α	US 5 119 412 A (ATTALLAH ARNALDO) 1992	1,3					
	siehe Zusammenfassung siehe Spalte 1, Zeile 1 - Spalte	5, Zeile					
	44 siehe Spalte 9, Zeile 17 - Spalte Zeile 2						
		_					
	-	/					
Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen Siehe Anhang Patentfamilie							
 Besondere Kategorien von angegebenen Veröffentlichungen "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "T" Spätere Veröffentlichung, die nach deminternationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der 							
"E" älteres Anme	Dokument, das jedoch erst am oder nach dem internationalen Idedatum veröffentlicht worden ist	Erfindung zugrundeliegenden Prinzips Theorie angegeben ist	3 3				
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden "V" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung von besonderer Bedeutung von besonderer Bedeut							
ausgeführt) Kann nicht als auf erinderischer i augkeit berunend betrachtet werden wenn die Veröffentlichung mit einer oder mehreren anderen							
"O" Veröffentlichung, die sich auf eine mundliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach "P" Veröffentlichung die State "P" Veröffentlichung die							
	dem beanspruchten Prioritätsdatum veröffentlichtworden ist av Veröffentlichung, die Mitglied derseiben Patentiamilie ist Datum des Abschlusses der internationalen Recherche Absendedatum des internationalen Recherchenberichts						
10.Juni 1998 17/06/1998							
Name und f	Name und Postanschrift der Internationalen Recherchenbehörde Bevollmächtigter Bediensteter						
	Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lievens, K	-				

INTERNATIONALER RECHERCHENBERICHT

Interna ales Aktenzeichen
PCT/EP 97/06663

C.(Fortsetz	ung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		7/00003
Kategorie'	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht komme	enden Teile	Betr. Anspruch Nr.
		enden Teile	Betr. Anspruch Nr.

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichung..., die zur selben Patentfamilie gehören

Intern: ales Aktenzeichen
PCT/EP 97/06663

	lm Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
FR	2680592	А	26-02-1993	JP 5054207 A JP 5061508 A DE 4212200 A	05-03-1993 12-03-1993 25-02-1993
DE	4325459	Α	09-02-1995	KEINE	
US	5119412	Α	02-06-1992	KEINE	
EP	0637004	Α	01-02-1995	NL 9301271 A AT 158432 T CA 2128355 A DE 69405664 D DE 69405664 T DK 637004 T EP 0775991 A ES 2107090 T	16-02-1995 15-10-1997 21-01-1995 23-10-1997 19-03-1998 14-04-1998 28-05-1997 16-11-1997